Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 4 (2023)

Bayesian Regularization (BR) Optimization Based DDoS Detection for SDN and Next Generation Communication Network

[1]Shekhar Nigam, [2]Dr. Sanjay Kumar Tiwari

[1]Phd Scholar, Dept. Computer Science and Engineering (CSE)
SunRise University, Alwar, Rajasthan , India
[2]Professor, HOD, dept. Computer Science and Engineering (CSE)
[2] SunRise University, Alwar, Rajasthan , India

E-mail – [1]shekhar_n2000@yahoo.com, [2]skt008@gmail.com[2]

Abstract: The rapid evolution of communication networks, particularly Software-Defined Networking (SDN) and next-generation communication infrastructures, has introduced new challenges in securing these dynamic and complex environments. Among the most persistent threats are Distributed Denial of Service (DDoS) attacks, which can disrupt critical services and inflict severe economic and operational damages. To combat these threats, novel and adaptive DDoS detection mechanisms are crucial. This paper proposes a Bayesian Regularization (BR) optimization-based approach for DDoS detection in SDN and next-generation communication networks. Bayesian Regularization is a statistical technique that combines the strength of Bayesian analysis with optimization methodologies, enabling the model to adapt to changing network conditions and attack strategies. This approach leverages the inherent advantages of SDN, such as centralized control and real-time network monitoring, to enhance the accuracy and timeliness of DDoS detection.

Keywords: SDN, Distributed Denial of Service (DDoS), Generation Communication Network, Bayesian regularization (BR)

1. INTRODUCTION

As the digital landscape continues to evolve, the security of communication networks becomes a paramount concern. In particular, Distributed Denial of Service (DDoS) attacks have emerged as a significant threat, disrupting services and causing financial losses for organizations[2][3]. Software-Defined Networking (SDN) and next-generation communication networks provide the agility and flexibility required for modern network management. However, with these advancements come new challenges in ensuring network security and reliability.

DDoS attacks involve overwhelming a target network or service with a flood of malicious traffic, rendering it inaccessible to legitimate users. Traditional methods for detecting and mitigating DDoS attacks often fall short in the dynamic environments of SDN and next-generation communication networks. To address this, innovative solutions are needed to adapt to the changing nature of DDoS attacks and provide robust protection[1].

Bayesian Regularization (BR) Optimization offers a promising approach for enhancing DDoS detection and mitigation in SDN and next-generation networks. This method leverages Bayesian statistics to model and predict network traffic behavior while simultaneously applying regularization techniques to improve the reliability of these predictions. The combination of probabilistic modeling and regularization aims to distinguish between normal and malicious traffic effectively[4][5].

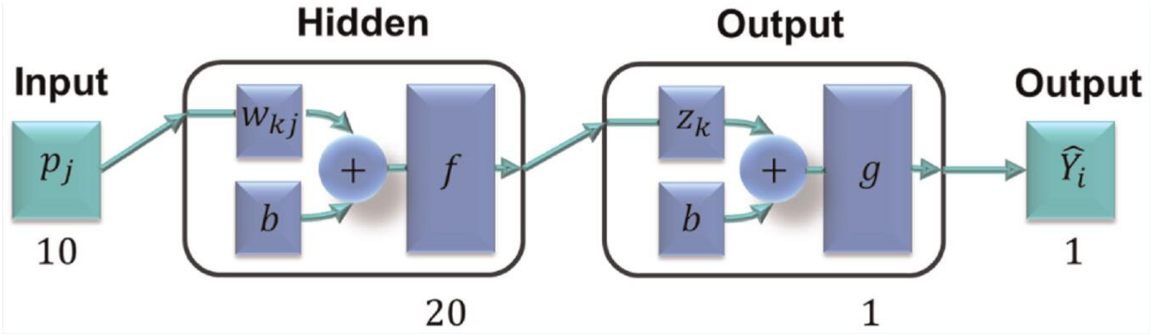


Fig 1: Bayesian Regularization

In the above fig. 1 shows Bayesian regularization is a method used to combat over fitting by incorporating Bayesian principles into the training process of neural networks. The key idea is to impose prior beliefs on the network's parameters, which helps constrain the learning process and prevent the model from fitting the noise in the data.

In the above section, I introduce the proposed research work background, discuss the cloud computing and d-dos attacks and the Bayesian regularization (BR) method is an important. in section ii, we will discuss dos attacks and their types. the next section-iii, discusses the previous works that were presented by different researchers. Bayesian regularization method IV Finally, describe the DDoS attack detection and prevention method presented in Section V. Section VI discusses the simulation and results of the proposed method. Last but not least, discuss the conclusion in section VII.

2. LITERATURE REVIEW

In this section, we will discuss the review of literature on cloud computing and also the different J48, Random Forest (RF), (SVM), and K-Nearest Neighbor, methods for the prevision of cloud computing. In the latest *Mustapha, et.al. [2023]* DDoS detection remains a challenging problem in cyber security. Recently, they have witnessed increasing interest in DDoS detection using machine learning (ML) and deep learning (DL) algorithms. Ironically, although ML/DL can increase detection accuracy, they can still be evaded by using ML/DL techniques to create attack traffic. authors addresses the above aspects of ML-based DDoS detection and anti-detection techniques. [1]. *Javaheri, et.al. [2023]* the current research Albeit rapid advances in information technology and artificial intelligence has offered many facilities, including ease of access and high availability, they caused a paradigm shift in cyber security threats. The large number of daily cyber-attacks indicates that computer systems and networks are highly vulnerable to cyber security threats. Anomaly detection systems have played a critical role in the security of organizations and businesses by finding new and Zero-day malicious behavior [2]. *Khedr, et.al. [2023]* internet of Things (IoT) have made security and privacy concerns more acute. Attacks such as distributed denial of service (DDoS) are becoming increasingly widespread in IoT, and the need for ways to stop them is growing. The use of newly formed Software-Defined Networking (SDN) significantly lowers the computational burden on IoT network nodes and makes it possible to perform more security measurements. This paper proposes an SDN-based, four-module DDoS attack detection and mitigation framework for IoT networks called FMDADM. The proposed FMDADM framework efficiently detects DDoS attacks at high and low rates, can discriminate between attack traffic and flash crowds, and protects both local and remote IoT nodes by preventing infection from propagating to the ISP level. The FMDADM outperformed most existing cutting-edge approaches across ten different evaluation criteria [3]. *Beitollahi, Hakem, et.al. [2022]* distributed denial of service (App-DDoS) attack, zombie computers bring down the victim server with valid requests. Intrusion detection systems (IDS) cannot identify these requests since they have legal forms of standard TCP connections. Researchers have suggested several techniques for detecting App-DDoS traffic. There is, however, no clear distinction between legitimate and attack traffic. In this paper, we go a step further and propose a Machine Learning (ML) solution by combining the Radial Basis Function (RBF) neural network with the cuckoo search algorithm to detect App-DDoS traffic. We begin by collecting training data and cleaning them, then applying data normalizing and finding an optimal subset of features using the Genetic Algorithm (GA) [4]. *Yungaicela-Naula et.al. [2022]* this software defined Distributed Denial-of-Service (DDoS) attacks are difficult to mitigate with existing defense tools. Fortunately, it has been demonstrated that Software-Defined

Networking (SDN) with machine learning (ML) and deep learning (DL) techniques has a high potential to handle these threats effectively. However, although there are many SDN-based solutions for detecting DDoS attacks, only a few contain mitigation strategies. Additionally, most previous studies have focused on solving high-rate DDoS attacks. For the time being, recent slow-rate DDoS threats are hard to detect and mitigate. In this work, we propose a modular, flexible, and scalable SDN-based framework that integrates a DL-based intrusion detection system (IDS) and a deep reinforcement learning (DRL)-based intrusion prevention system (IPS) to address slow-rate DDoS threats IDS achieved an average detection rate of 98%, with a flow sampling rate of 30%. In addition, IPS timely mitigated slow-rate DDoS with 100% of success for a few attackers [5]. *Valdovinos, et.al. [2021]* Software-defined networking (SDN) is a network paradigm that decouples control and data planes from network devices and places them into separate entities. In SDN, the controller is responsible for controlling the logic of the entire network while network switches become forwarding elements that follow rules to dispatch flows. There are, however, several limitations in such a paradigm, as compared to conventional networking. For example, the controller is sensitive to a broad range of attacks, including distributed denial of service (DDoS) attacks [6]. Bhayo, Jalal *et.al [2021]* Internet of Things (IoT) devices increases, the security threats and vulnerabilities associated with these resource-constrained IoT devices also rise. One of the major threats to IoT devices is Distributed Denial of Service (DDoS). To make the security of IoT devices effective and resilient, continuous monitoring and early detection, along with adaptive decision making, are required. These challenges can be addressed with software-defined networking (SDN), which provides an opportunity for effectively managing the DDoS threats faced by IoT devices. the results and comparative analysis, the proposed framework detects DDoS attacks in the early stage with high accuracy and detection rate from 98% to 100%, having a low false-positive rate [7].*Tuan, et.al. [2020]* in the research presented here, Botnet is regarded as one of the most sophisticated vulnerability threats nowadays. A large portion of network traffic is dominated by Botnets. Botnets are conglomeration of trade PCs (Bots) which are remotely controlled by their originator (BotMaster) under a Command and-Control (C&C) foundation. They are the keys to several Internet assaults like spams, Distributed Denial of Service Attacks (DDoS), rebate distortions, malwares and phishing. To over the problem of DDoS attack, various machine learning methods typically Support Vector Machine (SVM), Artificial Neural Network (ANN), Naïve Bayes (NB), Decision Tree (DT), and Unsupervised Learning (USML) (K-means, X-means etc.) were proposed. With the increasing popularity of Machine Learning in the field of Computer Security, it will be a remarkable accomplishment to carry out performance assessment of the machine learning methods given a common platform. [8]. *Frazao, et.al [2019]* Denial of Service attacks, which have become commonplace on the Information and Communications Technologies domain, constitute a class of threats whose main objective is to degrade or disable a service or functionality on a target. The increasing reliance of Cyber-Physical Systems upon these technologies, together with their progressive interconnection with other infrastructure and/or organizational domains, has contributed to increase their exposure to these attacks, with potentially catastrophic consequences. Despite the potential impact of such attacks, the lack of generality regarding the related works in the attack prevention and detection fields has prevented its application in real-world scenarios [13]. *D'Cruze, et.al [2018]* Distributed Denial of Service (DDoS) attacks are a common threat to network security. Traditional mitigation approaches have significant limitations in addressing DDoS attacks. authors reviews major traditional approaches to DDoS, identifies and discusses their limitations, and proposes a Software-Defined Networking (SDN) model as a more flexible, efficient, effective, and automated mitigation solution. They study focuses on Internet Service Provider (ISP) networks and uses the SDN security implementation at Verizon networks as a case study [14].

3. DENIAL-OF-SERVICE (DOS) ATTACK

In this section, we discuss the DoS attack in the cloud OSI model. Denial-of-service (DoS) attacks [9] involve resource stacking to make a system inaccessible to service requests [3]. As with DDoS attacks [18][19], these attacks are launched from a huge number of infected and controlled host devices. DDoS [26][27]assaults use botnets to fully disable a website or online service. They achieve this by flooding the target with activity from hundreds or even thousands of botnet devices [4]. Multiple hacked computers are used as attack traffic sources in DDoS operations. As if unanticipated traffic congestion were choking up the internet as well as the intranet, preventing ordinary internet network traffic from reaching their destinations, a DDoS assault would be like that. In the below fig. 2 shows the DDoS attack [10][12] on different layer.

3.1 TCP SYN Flood Attacks:

An attacker [17] utilises the buffer space after the first handshake of a Transmission Control Protocol (TCP) connection to perform a TCP SYN flood attack [22][23].

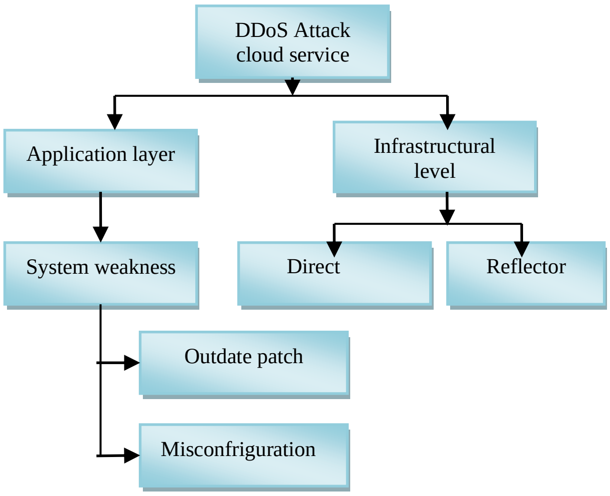


Figure 2: Denial of Service (DoS) attack in the cloud network [22]

In the next section, we will discuss the previous research studies and present research work in the areas of caber attacks and D-DoS attacks [21].

4. BAYESIAN REGULARIZATION METHOD

The Bayesian regularization learning method and BPNNs are neural networks that use back propagation to learn are discussed in this section. Demuth et al. [33] provides a more in-depth explanation. Improved generalization and minimum over-fitting of the training networks are achieved using a Bayesian regularization back propagation neural network. Neural networks may be trained using D, an input and target vector pair training data set for the network model.

$$D = \{(u_{1,}z_{o1}),(u_{2,}z),\ldots,(u_{nt,}Z_{ont})\}$$

The error e is calculated for every key (u) toward the system based on the difference between the goal output and the projected output. It is necessary to use a quantitative metric to assess the network's performance, i.e. how well it is able to match the test data. This metric is known as the network performance index, and it is used to improve the characteristics of the network. The sum of squared errors (SSE) governs the standard performance index F():

Training algorithm Using Bayesian Regularization Algorithm

$1.\, F(\overline{w}) = E_D = \sum_{i=1}^{nt}(ei)2 = \sum_{i=1}^{nt}(z_{oi} - a_{oi})T(z_{oi} - a_{oi})$

$2.\, F(\overline{w}) = \mu\overline{w}^T\overline{w} + vE_D = \mu E_w + vE_{D,}$

V is the regularization parameter and indicates the sum of SSW.

3. $P(\overline{w}|D, \mu, v, M_N = \frac{P(D|w,v,M_N)\ P(w|\mu M_N)}{P\ (D\backslash \mu,V,M_N)}$

4. $P\ (D|\overline{w}, \mu, v, M_N\ ) = \frac{\exp\ (-vE_D)}{Z_D(v)}$

Where $Z_D = (\pi/v)$ Q/2,

5.Q = $n_t \times N^{n1}$,

Prior to prior probability density, assuming a Gaussian distribution for the weights of a network, P $(\overline{w}|\mu, M_N)$is

given as:

6. $P(\overline{w}|\mu, M_N) = \frac{\exp(-\mu E_w)}{Z_w(\mu)}$

Where Z_w = (π/α)K/2

7. $P(\overline{w}|D, \mu, v, M_N) = \frac{\exp(-\mu E_w - vE_D)}{Z_F(\mu,v)} = \frac{\exp(-F(w))}{Z_F(\mu,v)}$,

At the point when$Z_F(\mu, v) = Z_D(v)Z_w(\mu)$ the normalizing factor is a constant.

8. $P(\mu, v|D, M_N) = \frac{P(D|\mu,v,M_N)\ P(\mu,v|M_N)}{P(D|M_N)}$

9. $\mu^* = \frac{\gamma}{2E_w(\overline{w}^*)}$ and $v^* = \frac{Q-\gamma}{2E_D\overline{w}^*)}$

10. $\gamma = K - \mu^*$tr$(H^*)^{-1}$, for 0$\leq \gamma \leq K$,

11. $H^* \approx J^T J$,

$z_F(\mu, v)$ shows that

12. $Z_F(\mu, v) \approx (2\pi)^{\frac{K}{2}}(\det(H^*))^{-\frac{1}{2}}\exp(-F(\overline{w}^*))$

$\overline{13. w}^{k+1} = \overline{w}^k - [J^T J + \curlywedge I]^{-1} J^T e$,

---

J^Te is the error gradient.

---

5. PROPOSED METHODOLOGY

In this section, we will discuss the proposed method. The key objective of a Distributed Denial of Service [29] (D-DoS) attack is to compile multiple systems across. The Internet is filled with agents and bot nets of networks. In the system model, the recognition module is compared to other strategies that use RBF networks with PSO-optimized training. This proposed research work implements an artificial neural network based on a modified cascaded [15] feed forward neural with an improved regression and optimised training Levenberg-Marquardt approach.

The overall complete method will be divided into three sections: training, testing, and validation. To implement the proposed method, we need to improve the raw data that is currently available. First, improve the data set manual. There are many entities available in the data set, but there is no utilization of the data. The initial data set is too large, so it is divided into three parts.

5.1 Training Bayesian Regularization

Bayesian Because the models are resilient and the validation procedure, which in standard regression methods grows as O(N2), is not required, Bayesian Regularization-based artificial neural networks (BRANNs) have a significant advantage over other regression techniques. The first method for improving generalization is called regularization.

Performance Function Modification

The mean sum of squares of network errors is a common way to measure how well feed forward neural networks are trained.

$$F = MSE = \frac{1}{N}\sum_{i=1}^{N}(e_i)^2 \tag{7}$$

$$= \frac{1}{N}\sum_{i=1}^{N}(t_i - a_i)^2 \tag{8}$$

The generalisation of the system may be improved by modifying the performance measure and including a term that consists of the mean of the sum of squares of the weights and biases of the system in the equation.

$$mse_{reg} = \gamma_{mse} + (1-\gamma) \times msw \tag{9}$$

Where γ is the performance ratio and mean square weight (msw),

$$msw = \frac{1}{n}\sum_{j=1}^{N}(w_j)^2$$

(10)

With the help of this reward function, as well as the lowered weights and biases that come with it, a better and less likely to over fit system response can be made possible.

5.2 Cascade-Forward Neural Network

A network with direct connections between the input and output layers is generated if the perception and multilayer network are joined besides the connection indirectly. The network formed from this connection pattern is called Cascade Forward Neural Network (CFNN). The CFNN model generates the following sets of equations:

$$y = \sum_{i=1}^{n} f^i * \omega_t^i \chi_i + f^0\left(\sum\nolimits_{j=1}^{n} f^i * \omega_j^0 \left(\sum\nolimits_{i=1}^{n} \omega_{ji}^h \chi_i\right)\right)$$

(11)

Where f^i is the activation function from the input layer to the output layer and is ω is weight from. The transitions from the input layer or the output layer are presented. If a bias is introduced into the input layer and the activation function of each neuron in the hidden layer is calculated, the formula for the hidden units is obtained (5) becomes

$$y = \sum_{i=1}^{n} f^i * \omega_t^i \chi_i + f^0\left(\omega^b \sum\nolimits_{j=1}^{n} f^i * \omega_j^0 \left(\omega_j^b + \sum\nolimits_{i=1}^{n} \omega_{ji}^h \chi_i\right)\right)$$

(12)

The CFNN model is used to analyses time series data in this study. There are delays of Xt-1, Xt-2, and so on in the input layer while actual data Xt is produced from neurons in the output layer. In the below fig. 3 shows the standard architecture of the cascaded feedforward neural network and fig 4 shows raw data processing algorithms steps.

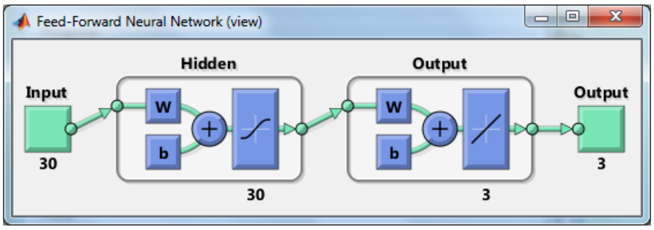


Fig 3: Cascaded Feed forward Neural Network

6. SIMULATION AND RESULTS

In this section, we are describing the implementation details and designing issues for our proposed research work. By searching, we have observed that for our proposed work, MATLAB 2020 is the well-known platform to perform the suggested approach. We tend to perform some experimental tasks in MATLAB 2020b code, and additionally, the well-noted DDoS data set by the Canadian Institute of Cyber security (CICIDS2017) is provided by the Canadian Institute [10]. This chapter is split into three major halves. The initial one describes the summary of the MATLAB surroundings, the other is to explain the CICIDS2017 information sets used for implementation, and the last section outlines all the tables, snapshots, and graphs employed in our planned work.

6.1 Data set

The Canadian Institute of Cybersecurity (CICIDS2017) Intrusion Detection Evaluation Dataset is utilized for design training and evaluation [20]. Numerous threats, such as DDoS as well as botnet activity are documented in the report. We used the DoS data set as the basis for our classification model in this study. There are 84 variables in each flow record in the CICIDS 2017 dataset, which is in comma-separated (.CSV) format. In the below fig. 5 shows DDOS Attack Data Sheet file in Matrix Laboratory 2020

6.2 Result Parameters

The strategy described here examines a variety of outcome characteristics. Here are the variables you'll want to keep an eye on.

1. True Positive (T.P.): A true positive is an event in which the model accurately predicts the positive class. A genuine positive is when researchers verify the effectiveness of a result that is in line with what was expected [16].
2. False Negative (F.N.): A test result that incorrectly suggests that a condition does not hold is known as a false negative error. When a test result wrongly suggests the absence of a disorder, a negative test occurs [10].
3. False Positive (F.P.): When the values predict the positive class wrongly, it creates a false positive. Mistakes in the binary classification result in wrongly diagnosing a disorder as a false positive [20].
4. True Negative (T.N.) : Models that accurately forecast the class of negative outcomes known as "genuine negatives" [11].
5. Accuracy (Acc) [25]: Accuracy is the key parameter for the performance calculation of the presented work. It’s a combination of true positive, true negative, false positive, and false negative. Accuracy is inversely proportional to sensitivity; it's the summation of the TP, TN, FP, and FN.

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \tag{13}$$

6. Confusion Matrix (C.M.): Machine learning model predictions are compared with real target numbers in a matrix. The columns represent the target variable's expected values.

6.3 Results Outcomes

The result outcomes of the proposed method are shown below in terms of different results parameters as well as in the form of nn train tool outcomes images. There's a neural network (NN) experiment depicted in fig. (6). As we already discussed, the training weight optimizer utilised is Bayesian Regularization and performance error calculations are in terms of mean square error. A total of thirty input features are used in this algorithm. The complete process takes 30 iterations; total time in training is 2 minutes and 4 seconds in 8-core parallel processing. If processed in serial processing, it takes 30 mins to process. The other result parameters are gradient and mu. TABLE I, discuss the proposed method cascaded [15] feed forward validation outcomes.

Table 1: Training Input Parameters of Proposed Cascaded Forward Network Using BR Algorithm (FFN - BR)

S.No.	Parameters Name	Inputs of Parameter
01	Data Division	Random
02	Network Type	**Cascaded Forward (CF)**
03	Training	**Bayesian regularization**
04	Performance	Mean square Error (MSE)

TABLE 2: PROPOSED CASCADED FEED FORWARD BR RESULTS

S.No.	Parameters Name	Inputs of Parameter	Training Outputs
01	Number of Epochs	0-30	30 iterations
02	Time	12min 22 sec	12 min 22 sec
03	Performance	**4.64**	**0.000681**
04	Gradient	8.72	0.0122
05	Effective Parameter	1.11e+03	1.01e+03
06	Sum Squared Param	168	126

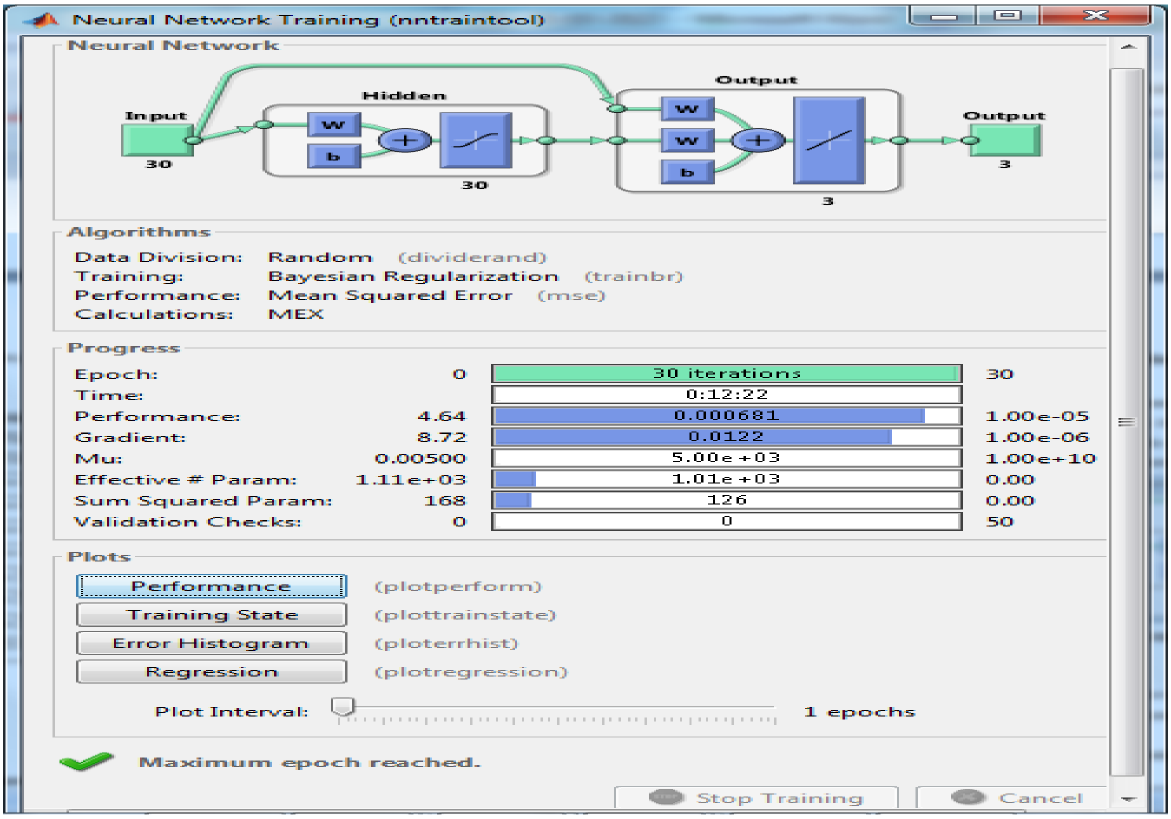
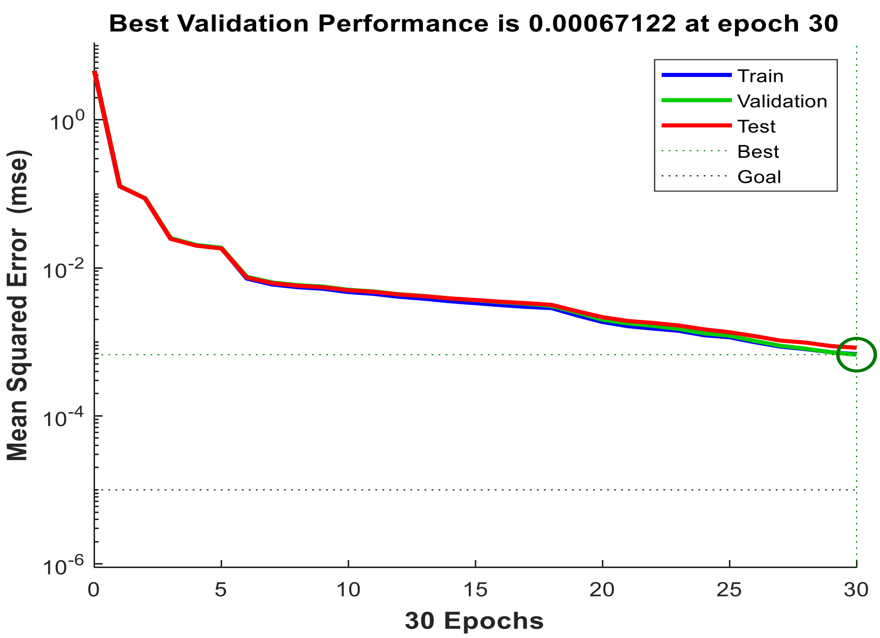
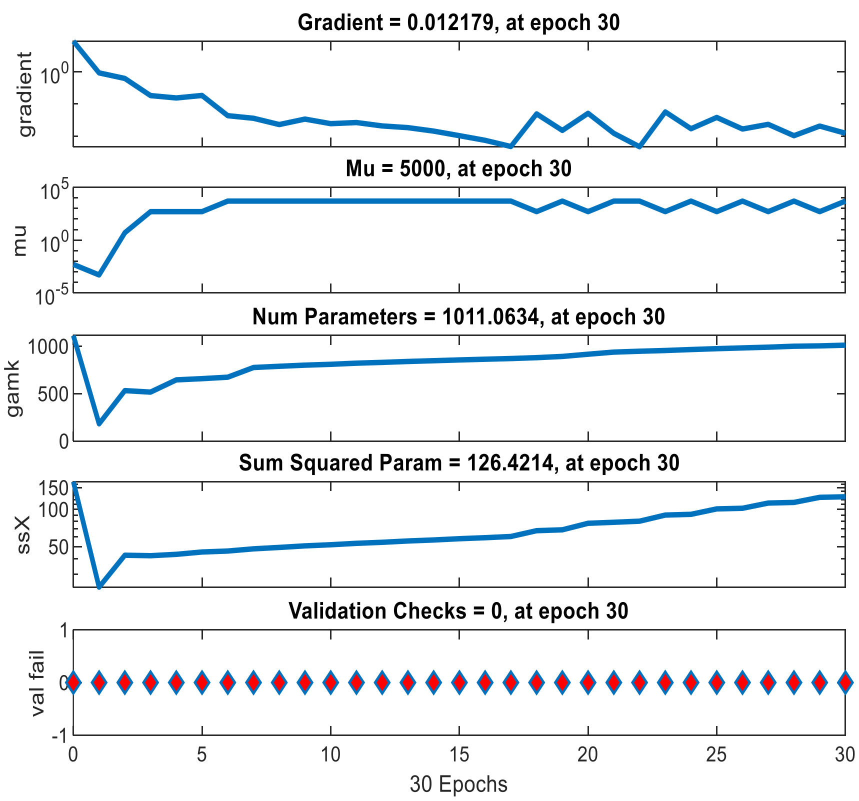


Fig 4: neural network simulation model



(a) the result training and performance validation



(b) Shows the gradient (G), mu, gamk

Fig 5: Error Histogram analysis of proposed Bayesian Regularization cascaded forward method

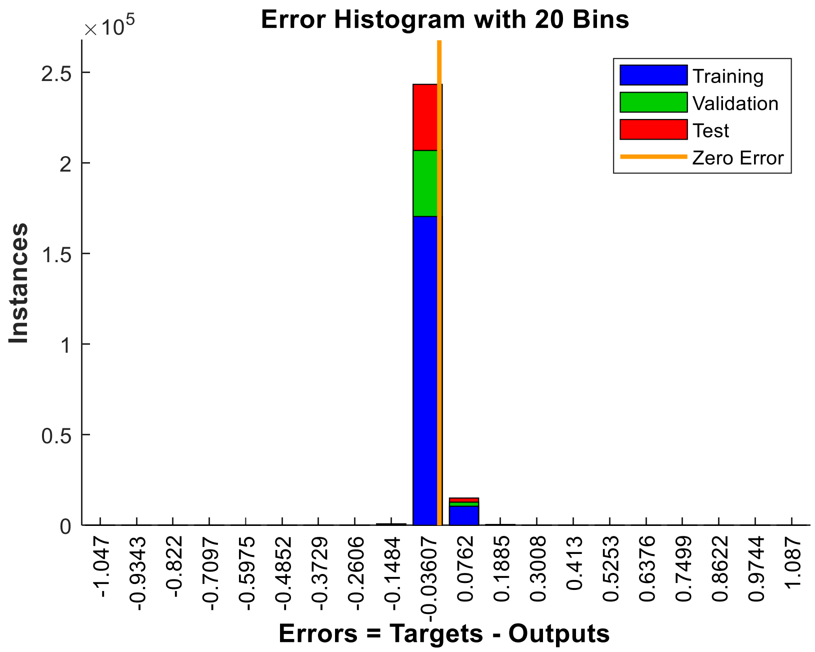
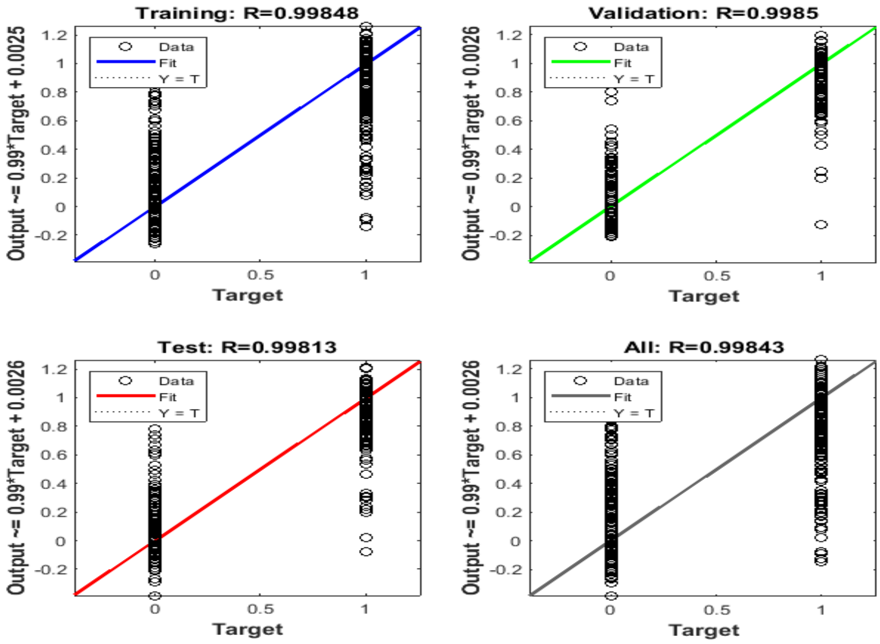


Fig 6: Error Histogram analysis of proposed Bayesian Regularization cascaded forward method



(c) Shows the Train, test and validation

Fig.7: Shows the performance of proposed Cascaded Feed Forward NN network

In the above figure 7 shows the performance outcomes of proposed cascaded feed forward NN network. In the above fig 7 (a) describe the validation performance, 7 (b) shows the gradient (G) outcome of proposed method and last fig. 7(c) shows the regression plots of training, testing and validation.

TABLE 3: RESULT COMPARISON OF DIFFERENT METHODS

S. No.	Year / Ref	Method	Type of ANN	Accuracy	Data set
01	2023/ Presented	Bayesian Regularization + Cascaded feed forward network	Machine Learning	**99.90%**	CICIDS2017
02	2022 /[8]	CNN and LSTM	Deep Learning	99.03%	CICIDS2017

7. CONCLUSION

The process has been demonstrated that they may be dispersed around various regions and employed for both observation and carrying out an assault. These kind of cyber attacks will continue to get deadlier in coming years because to the rapid development of Network of Issues connections. Due to the wide range of applications it can serve, the Web of objects, often known as the Internet of Things, is swiftly taking over as the primary communication method. There is an increasing demand for platforms that can fight versus denial of service attacks, which are a type of global denial of service attack that are becoming more prevalent in the IoT setting.

REFERENCES

JOURNAL

[1] Mustapha, Ali, Rida Khatoun, Sherali Zeadally, Fadlallah Chbib, Ahmad Fadlallah, Walid Fahs, and Ali El Attar. "Detecting DDoS attacks using adversarial neural network." Computers & Security 127 (2023): 103117.

[2] Javaheri, Danial, Saeid Gorgin, Jeong-A. Lee, and Mohammad Masdari. "Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives."Information Sciences (2023).

[3] Khedr, Walid I., Ameer E. Gouda, and Ehab R. Mohamed. "FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks." IEEE Access 11 (2023): 28934-28954.

[4] Beitollahi, Hakem, Dyari Mohammed Sharif, and Mahdi Fazeli. "Application layer DDoS attack detection using cuckoo search algorithm-trained radial basis function." IEEE Access 10 (2022): 63844-63854.

[5] Yungaicela-Naula, Noe M., Cesar Vargas-Rosales, Jesús Arturo Pérez-Díaz, and Diego Fernando Carrera. "A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning." Journal of Network and Computer Applications 205 (2022): 103444.

[6] Valdovinos, Ismael Amezcua, Jesús Arturo Pérez-Díaz, Kim-Kwang Raymond Choo, and Juan Felipe Botero. "Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions." Journal of Network and Computer Applications 187 (2021): 103093.

[7] Bhayo, Jalal, Riaz Jafaq, Awais Ahmed, Sufian Hameed, and Syed Attique Shah. "A time-efficient approach toward DDoS attack detection in IoT network using SDN." IEEE Internet of Things Journal 9, no. 5 (2021): 3612-3630.

[8] Tuan, Tong Anh, Hoang Viet Long, Le Hoang Son, Raghvendra Kumar, Ishaani Priyadarshini, and Nguyen Thi Kim Son. "Performance evaluation of Botnet DDoS attack detection using machine learning." Evolutionary Intelligence 13 (2020): 283-294.

[9] Bawany, N.Z., Shamsi, J.A. and Salah, K., 2017. DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arabian Journal for Science and Engineering, 42(2), pp.425-441.

[10] Hoque, Nazrul, Dhruba K. Bhattacharyya, and Jugal K. Kalita. "Botnet in DDoS attacks: trends and challenges." IEEE Communications Surveys & Tutorials 17, no. 4 (2015): 2242-2270.

[11] Ashraf, Javed, and Seemab Latif. "Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques." In 2014 National software engineering conference, pp. 55-60. IEEE, 2014.

[12] Choi, Junho, Chang Choi, Byeongkyu Ko, and Pankoo Kim. "A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment." Soft Computing 18, no. 9 (2014): 1697-1703.

CONFERENCE

[13] Frazão, Ivo, Pedro Henriques Abreu, Tiago Cruz, Hélder Araújo, and Paulo Simões. "Denial of service attacks: Detecting the frailties of machine learning algorithms in the classification process." In Critical Information Infrastructures Security: 13th International Conference, CRITIS 2018, Kaunas, Lithuania, September 24-26, 2018, Revised Selected Papers 13, pp. 230-235. Springer International Publishing, 2019.

[14] D'Cruze, Hubert, Ping Wang, Raed Omar Sbeit, and Andrew Ray. "A software-defined networking (SDN) approach to mitigating DDoS attacks." In Information Technology-New Generations: 14th International Conference on Information Technology, pp. 141-145. Springer International Publishing, 2018.

[15] Yang, Lingfeng, and Hui Zhao. "DDoS attack identification and defense using SDN based on machine learning method." In 2018 15th international symposium on pervasive systems, algorithms and networks (I-SPAN), pp. 174-178. IEEE, 2018.

[16] Zekri, M., El Kafhali, S., Aboutabit, N. and Saadi, Y., 2017, October. DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd international conference of cloud computing technologies and applications (CloudTech) (pp. 1-7). IEEE.

[17] Agarwal, Mayank, Dileep Pasumarthi, Santosh Biswas, and Sukumar Nandi. "Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization." International Journal of Machine Learning and Cybernetics 7, no. 6 (2016): 1035-1051.

[18] Yusof, Ahmad Riza'ain, Nur IzuraUdzir, and Ali Selamat. "An evaluation on KNN-SVM algorithm for detection and prediction of DDoS attack." In International conference on industrial, engineering and other applications of applied intelligent systems, pp. 95-102. Springer, Cham, 2016.

[19] Bhatia, Sajal. "Ensemble-based model for DDoS attack detection and flash event separation." In 2016 Future Technologies Conference (FTC), pp. 958-967. IEEE, 2016.

[20] Mousavi, Seyed Mohammad, and Marc St-Hilaire. "Early detection of DDoS attacks against SDN controllers." In 2015 international conference on computing, networking and communications (ICNC), pp. 77-81. IEEE, 2015.

[21] Balkanli, Eray, Jander Alves, and A. Nur Zincir-Heywood. "Supervised learning to detect DDoS attacks." In 2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), pp. 1-8. IEEE, 2014.

[22] Darwish, Marwan, Abdelkader Ouda, and Luiz Fernando Capretz. "Cloud-based DDoS attacks and defenses." In International Conference on Information Society (i-Society 2013), pp. 67-71. IEEE, 2013.

[23] Kumar, Naresh, and Shalini Sharma. "Study of intrusion detection system for DdoS attacks in cloud computing." In 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1-5. IEEE, 2013.

[24] Ansarinia, Morteza, Seyyed Amir Asghari, Afshin Souzani, and AhmadrezaGhaznavi. "Ontology-based modeling of DDoS attacks for attack plan detection." In 6th International Symposium on Telecommunications (IST), pp. 993-998. IEEE, 2012.

[25] Beitollahi, Hakem, and Geert Deconinck. "Tackling application-layer DDoS attacks." Procedia Computer Science 10 (2012): 432-441.

[26] Suresh, Manjula, and R. Anitha. "Evaluating machine learning algorithms for detecting DDoS attacks." In International Conference on Network Security and Applications, pp. 441-452. Springer, Berlin, Heidelberg, 2011.

[27] Srivastava, A., B. B. Gupta, A. Tyagi, Anupama Sharma, and Anupama Mishra. "A recent survey on DDoS attacks and defense mechanisms." In International Conference on Parallel Distributed Computing Technologies and Applications, pp. 570-580. Springer, Berlin, Heidelberg, 2011.

[28] Kokila, R. T., S. ThamaraiSelvi, and Kannan Govindarajan. "DDoS detection and analysis in SDN-based environment using support vector machine classifier." In 2014 Sixth International Conference on Advanced Computing (ICoAC), pp. 205-210. IEEE, 2014.

[29] Barati, Mehdi, Azizol Abdullah, Nur IzuraUdzir, RamlanMahmod, and Norwati Mustapha. "Distributed Denial of Service detection using hybrid machine learning technique." In 2014 International Symposium on Biometrics and Security Technologies (ISBAST), pp. 268-273. IEEE, 2014.

[30] Kumar, Naresh, and Shalini Sharma. "Study of intrusion detection system for DDoS attacks in cloud computing." In 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1-5. IEEE, 2013.